

IN THE CLAIMS

1. (Previously Presented) A method for time stamping a document comprising:
receiving a time stamp request at an outside agency at a first time, said time stamp request comprising identifying data associated with said document;
creating at said outside agency a time stamp receipt based on said identifying data and a time indication; and
generating at said outside agency a message authentication code based on said time stamp receipt and a secret key;
transmitting said time stamp receipt and said message authentication code to a designated party;
receiving a certification request at said outside agency at a second time, said certification request comprising said time stamp receipt and said message authentication code;
validating said message authentication code at said outside agency using said secret key;
and
certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said message authentication code is valid.
2. (Original) The time stamping method of claim 1 wherein said identifying data comprises a digital representation of at least a portion of said document.
3. (Original) The time stamping method of claim 2 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

4. (Original) The time stamping method of claim 3 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.
5. (Previously Presented) The time stamping method of claim 1 wherein said time stamp receipt comprises a copy of at least a portion of said identifying data concatenated with said time indication.
6. (Previously Presented) The time stamping method of claim 5 wherein said time stamp receipt comprises a digital sequence derived from said identifying data concatenated with said time indication.
7. (Previously Presented) The time stamping method of claim 1 wherein said time stamp request further comprises an identification number associated with the requestor.
8. (Original) The time stamping method of claim 1 wherein said message authentication code comprises a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenated together.
9. (Previously Presented) The time stamping method of claim 6 wherein the step of validating said message authentication code comprises recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code.

10. (Previously Presented) The time stamping method of claim 1 wherein the certifying step comprises signing said message authentication code using a private signature key controlled by said outside agency.

11. (Previously Presented) The time stamping method of claim 1 wherein the certifying step comprises signing said time stamp receipt using a private signature key controlled by said outside agency.

12. (Previously Presented) The time stamping method of claim 1 further comprising the step of storing said secret key in a database at said outside agency.

13. (Previously Presented) The time stamping method of claim 1 wherein each time stamp receipt comprises a sequential record number that is used at said outside agency to look up said secret key in said database.

14. (Previously Presented) The time stamping method of claim 1 further comprising the step of transmitting said certified time stamp receipt to said requestor.

15. (Previously Presented) A method for time stamping a document comprising:

receiving a time stamp request at an outside agency at a first time, said time stamp request comprising identifying data associated with said document;

creating at said outside agency a time stamp receipt based on said identifying data and a time indication;

generating at said outside agency a message authentication code based on said time stamp receipt and a first secret key;

encrypting the first secret key with a second secret key to generate a key message;

generating a second message authentication code based on said first message authentication code and said first secret key using a third secret key;

transmitting said time stamp receipt, said first message authentication code, said second message authentication code, and said key message to said requestor;

receiving at said outside agency at a second time a certification request, said certification request comprising said time stamp receipt, said first message authentication code, said second message authentication code, and said encrypted key message;

decrypting at said outside agency said encrypted key message to recover said first secret key;

validating said second message authentication code at said outside agency using said third secret key;

validating said first message authentication code at said outside agency using said first secret key if said second message authentication code is valid; and

certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said first message authentication code is valid.

16. (Original) The time stamping method of claim 15 wherein said identifying data comprises a digital representation of at least a portion of said document.

17. (Original) The time stamping method of claim 16 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

18. (Original) The time stamping method of claim 17 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

19. (Previously Presented) The time stamping method of claim 17 wherein said time stamp receipt comprises a copy of at least a portion of said identifying data concatenated with said time indication.

20. (Previously Presented) The time stamping method of claim 19 wherein said time stamp receipt comprises a digital sequence derived from said identifying data concatenated with said time indication.

21. (Previously Presented) The time stamping method of claim 15 wherein said time stamp request further comprises an identification number associated with the requestor.

22. (Previously Presented) The time stamping method of claim 15 wherein said first message authentication code comprises a numeric representation generated by application of a deterministic function to said time stamp receipt and said first secret key concatenated together.

23. (Previously Presented) The time stamping method of claim 22 wherein said second message authentication code comprises a numeric representation generated by application of a deterministic function to said first message authentication code concatenated with said first and third secret keys.

24. (Previously Presented) The time stamping method of claim 23 wherein the step of validating said second message authentication code comprises recomputing said second message authentication code at said outside agency using said first message authentication code received as part of said certification request, said second secret key and said third secret key, and comparing the recomputed second message authentication code to said received second message authentication code.

25. (Previously Presented) The time stamping method of claim 24 wherein the step of validating said first message authentication code comprises recomputing said first message authentication code at said outside agency using said time stamp receipt received as part of said certification request and said first secret key and comparing the recomputed first message authentication code to said received first message authentication code.

26. (Previously Presented) The time stamping method of claim 15 wherein the step of certifying said time stamp receipt comprises signing said first message authentication code using a private signature key controlled by said outside agency.

27. (Previously Presented) The time stamping method of claim 15 wherein the step of certifying said time stamp receipt comprises signing said time stamp receipt using a private signature key controlled by said outside agency.

28. (Previously Presented) The time stamping method of claim 15 further comprises the step of transmitting said certified time stamp receipt to said requestor.

29-46. (Cancelled).

47. (Previously Presented) The time stamping method of claim 1 wherein certifying said time stamp receipt at said outside agency comprises signing said time stamp receipt with a private signature key.

48. (Previously Presented) The time stamping method of claim 1 wherein certifying said time stamp receipt at said outside agency comprises signing said message authentication code with a private signature key.

49. (Previously Presented) The time stamping method of claim 15 wherein certifying said time stamp receipt at said outside agency comprises signing said time stamp receipt with a private signature key.

50. (Previously Presented) The time stamping method of claim 15 wherein certifying said time stamp receipt at said outside agency comprises signing said message authentication code with a private signature key.

51-52. (Cancelled).